Radware DefensePipe

General Instructions for customer

1. Introduction

This document describes Radware's DefensePipe cloud extension setup instructions for Radware customers.

Radware

Radware (NASDAQ: RDWR) is a global leader of application delivery and application security solutions for virtual and cloud data centers. Its award-winning solutions portfolio delivers full resilience for business-critical applications, maximum IT efficiency, and complete business agility. Radware's solutions empower more than 10,000 enterprise and carrier customers worldwide to adapt to market challenges quickly, maintain business continuity, and achieve maximum productivity while keeping costs down. For more information, visit www.radware.com.

Radware AMS

Radware's Attack Mitigation Solution protects the application infrastructure against network and application downtime, application vulnerability exploitation, malware spread, information theft, web service attacks, and web defacement. AMS is typically deployed in-line and processes all traffic directed at the protected service, hence it utilizes high network and application awareness. It maintains continuity of services and protects critical infrastructure from all contemporary cyber-threats.

DefensePipe

Recent trends in the threat landscape introduce an increase in extremely high-volume "Pipe Saturation" attacks, which require in-the-cloud protection. In order to cover this threat, Radware offers customers a service-based cloud protection, activated via their on-premises AMS.

The Unique AMS-DefensePipe Advantage

Utilizing high application awareness, achieved by processing all traffic directed to a protected service, AMS is able to stop the vast majority of attacks without the need to make any changes. This enables several advantages including:

- **Widest coverage** – From single packet vulnerability-based attacks to high-volume floods, AMS covers the entire range of threats.
- **Shortest time to protection** – Due to constant processing of the entire traffic by the on-premises mitigation device, AMS is able to detect and mitigate attacks in seconds.
- **Utilizing baselines** – Learning of traffic parameters, which is performed by the on-premises device is used in the cloud when the service is activated. This allows for higher detection and mitigation capability.
- **Traffic Diversion only on volumetric attacks** – The majority of attacks are blocked by the on-premises equipment. Traffic would be diverted to the cloud extension only under pipe-saturation risk, ensuring minimum routing changes and network overhead.
- **Single point of contact** – Radware ERT is the sole contact for attack mitigation.
- **Integrated reporting** – Reporting of on-premises and cloud mitigation is consolidated into a single report making incident management easy and convenient.

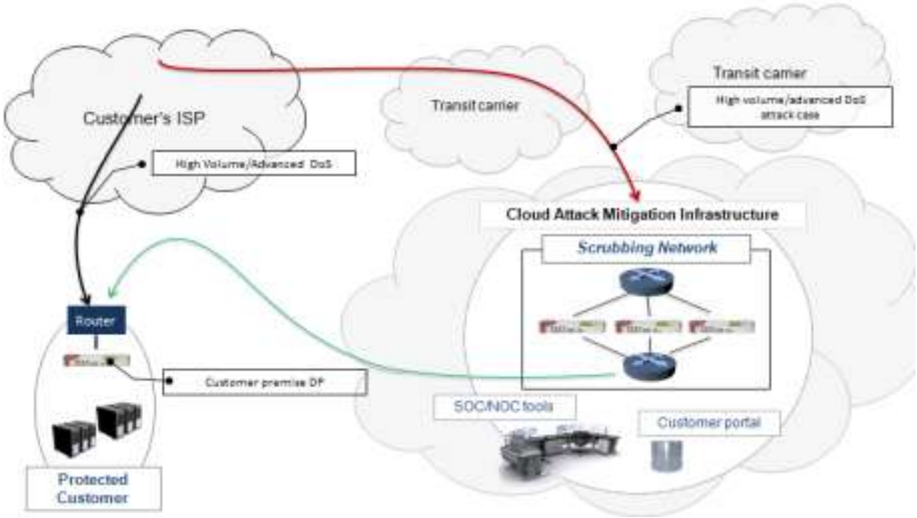


Figure 1: Illustration of cloud and customer-premises components in attack mitigation

2. Setup Mode

There are two possible setup procedures, depending on the customer status:

2.1. Emergency Setup

If you are under attack, you may purchase an accelerated setup, supported by Radware ERT. Please consult with your local Radware engineer for further details.

2.2. Normal (“Peacetime”) Setup

Under normal circumstances, the setup process is fully supported by Radware SE and is described below.

3. Choosing the Best Diversion Option

Under a volume attack, traffic targeted at the customer’s protected service/network will be diverted towards the cloud scrubbing-center infrastructure to be cleaned and routed back to the customer. The diversion can be done by two different methods: BGP or DNS. Each method has its advantages and limitations. Make sure you understand the different methods before selecting the method that is appropriate for your environment. In case of uncertainty, please consult with your local Radware engineer.

Once the appropriate method is chosen, the Radware SE will provide you with a setup form for the relevant diversion method.

3.1. BGP-based Diversion

General Advantages

- Traffic redirection is performed per network; therefore, this is a more complete protection.
- Requires less or no action on the customer side for traffic diversion under attack.

General Limitations/Prerequisites

- Requires the customer to own an AS of at least a /24 network segment.
- Requires an out-of-band GRE tunnel to be set up between the customer and the scrubbing center.

GRE Tunnel Setup

- Allocate router (GRE termination point) and IP address for GRE tunnel, as follows:
  - Publicly routable IP address for tunnel endpoint.
  - Not part of protected network (to be diverted using BGP).
  - Preferable – part of PA block by customer's ISP.
- Setup GRE tunnel between DefensePipe and your GRE router with:
  - Private network address (specified by DefensePipe).
  - Tunnel endpoints:
    - Source – your public IP address (see above).
    - Destination – public IP address specified by DefensePipe.
  - MTU = 1500
- (Optional) QoS for tunnel on main external interface.

There are three possible options for BGP-based diversion:

3.1.1. BGP Diversion – Smaller Prefix

Overview

With this method, under attack, DefensePipe will advertise the customer's IP address block using smaller prefixes (for example, two /24 blocks instead of /23 advertised by customer and ISP), thus taking precedence over customer's original route.

Prerequisites

- Block of IP addresses, at least /23.
- Public ASN.
- Active BGP peering with upstream ISP.

Advantages

- No action required on customer side for activation under attack.
- No change required to normal BGP settings.

Setup

Customer to provide:

- IP block (/23 or larger) for protected networks.
- ASN (for monitoring only).
- BGP peer (for monitoring only).

Activation

- No action required from customer.

Deactivation

- No action required from customer.

3.1.2. BGP Diversion – AS-Path Prepend

Overview

This method is recommended for customers who cannot use the “Smaller Prefix” method above. With this method, normal BGP advertisements made by the customer/ISP are modified to increase the AS path by few steps. Under attack, DefensePipe will begin advertising the customer’s IP address block with no extra steps in the AS Path, thus taking precedence over the original route because of the AS path length.

Prerequisites

- Block of IP addresses, at least /24.
- Public ASN.
- Active BGP peering with upstream ISP.

Advantages

- No action required on customer side for activation under attack.

Disadvantages

- Required to add a few steps to normal AS path settings.

Setup

Customer to provide:

- IP block (/24 or larger) for protected networks.
- ASN (for monitoring only).
- BGP peer (for monitoring only).

Change:

Customers should modify their own BGP advertisements to increase the AS path by at least an extra four steps.

Verify:

- Typical AS path via customer's ISP and via DefensePipe.
- Any AS-path limitations imposed by customer's ISP.

Example: For a customer with network 2.4.6.0/24 and ASN 12345:

- BEFORE - AS path looks like → 2.4.6.0/23 AS789 AS12345
- AFTER - AS path looks like → 2.4.6.0/23 AS789 AS12345 AS12345 AS12345 AS12345

Activation

- No action required from customer.

Deactivation

- No action required from customer.

3.1.3. BGP Diversion – Advertisement/Withdrawal

Overview

This method is recommended for customers who cannot use any of the previously described methods. Here, customers will have to withdraw their own BGP advertisements for DefensePipe BGP advertisements to take effect.

Prerequisites

- Block of IP addresses, at least /24.
- Public ASN.
- Active BGP peering with upstream ISP.

Advantages

- Not required to add steps to the normal AS path settings.

Disadvantages

- Action required on customer side for activation under attack (withdrawal).

Setup

Customer to provide:

- IP block (/24 or larger) for protected networks.
- ASN (for monitoring only).
- BGP peer (for monitoring only).

Activation

- Customer router and ISP should withdraw BGP advertisement of the protected network.

Deactivation

- Resume advertising protected networks from customer's router to the ISP.

3.2. DNS-based Diversion

Overview

This method is recommended for customers who do not comply with the above BGP prerequisites or require setup in an accelerated mode. The diversion is performed per service by changing the DNS record for the protected service under attack. The TTL on DNS records for the protected service is also reduced to ensure the diversion is quick enough.

General Advantages

- Simpler setup in cases of few protected services.

General Limitations/Prerequisites

- Protection is per service, so this does not apply for attacks on other network elements on the same segment.
- Requires an upstream ISP ACL setup to allow only scrubbing-center traffic under attack.
- Requires customer action at the activation stage.

Setup

For each server to be protected by DefensePipe, you should:

- Reduce the TTL for protected-servers' DNS record to 300 seconds or less.
- Receive from DefensePipe a "VIP" allocated to serve as an alternative target under attack.
- Enable access from the DefensePipe scrubbing center to the protected server's address.

Example:

- Old → www IN A 1.2.3.4
- New → www 300 IN A 1.2.3.4
  - Note: Per-record TTL overrides zone TTL.

Activation

- Change the protected server's DNS record to point to DefensePipe VIP.
  - Update the DNS A or CNAME record.
  - Update the DNS zone serial number to ensure propagation.
- It is recommended, to ensure pipe-saturation protection, to block by ACL all incoming Internet traffic to the protected server, except for traffic coming from the DefensePipe scrubbing center. This ACL is best applied at the upstream ISP router.

Deactivation

- Restore protected server’s DNS record to point to the original server, instead of DefensePipe VIP.
    - Update the DNS A or CNAME record.
    - Update the zone serial number to ensure faster propagation.
- Allow incoming traffic from Internet (if it was blocked).

4. Forwarding Required Information

- Gather the required information detailed in the setup form suitable for the diversion method chosen and forward the form to your local Radware SE.
- (BGP case only) Complete the provided BGP LOA form and forward it to your local Radware SE.

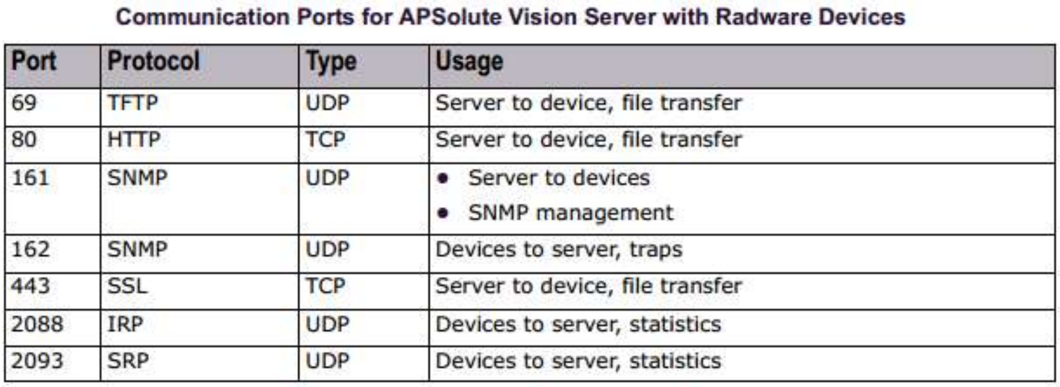
5. Receiving Information from Radware SE

Once information has been forwarded to Radware, you should quickly receive the required information to complete your side of the setup according to the selected diversion option.

6. Completing Setup Operations

Complete the following set-up operations:

6.1. Open the required IP addresses and ports in your FW to allow signaling between cloud management IP address received from DefensePipe and your DefensePro according to the following:



Communication Ports for APSolute Vision Server with Radware Devices

Port	Protocol	Type	Usage
69	TFTP	UDP	Server to device, file transfer
80	HTTP	TCP	Server to device, file transfer
161	SNMP	UDP	• Server to devices • SNMP management
162	SNMP	UDP	Devices to server, traps
443	SSL	TCP	Server to device, file transfer
2088	IRP	UDP	Devices to server, statistics
2093	SRP	UDP	Devices to server, statistics

6.2. Configure the cloud management IP address as a data-reporting destination on the local DefensePro:

- CLI: *dp reporting data-report address add <ip-address>*
- Vision: Advanced Parameters > Security Reporting Settings > Data Reporting Destinations > Add new destination

6.3. Make required changes to DNS servers/routers, as specified in the instructions above, to allow the diversion to take place.

6.4. Complete GRE tunnel set up changes.

Any assistance required in those steps should be discussed with your local Radware SE, who is able to bring DefensePipe representative online for further assistance.

Once the above changes are completed, a Radware SE will coordinate a setup-verification test with DefensePipe.

7. Setup-Verification Test

It is highly recommended that a Radware SE be onsite with you during the setup-verification test is performed.

The test will include:

Verification of DefensePro Signaling to Cloud Service

- Verify with DefensePipe that a ping is available from cloud management to the local DefensePro.
- Verify with DefensePipe that reporting is seen by the cloud.

Diversion of Traffic to the Cloud and Deactivation

- According to the configured diversion options, diversion actions will be performed and traffic will be diverted through the cloud.
- Verify that the protected asset is reachable from the Internet.

The verification test will be assisted by the DefensePipe NOC, which will be available by phone to assist the Radware SE in the test process.

The verification test concludes the setup procedure. From this moment onwards, the service is active.

8. DefensePipe Protection Activation

There are two methods by which the service may be activated:

8.1. ERT Activation

In the event of an attack that is not mitigated automatically by your DefensePro, invoke ERT through Radware Technical Support. Radware ERT will have a broader tool set—your being a DefensePipe customer, which includes the ability to divert traffic for cloud mitigation when needed.

8.2. Signaling Activation

Traffic monitoring signals may trigger an alert on the cloud-service systems, indicating that a high risk for saturation exists. Radware Technical Support will contact you to verify that activation is needed. If verified, ERT will be invoked and activate the service. This method requires a 24x7 contact.